IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

AMERICAN HEALTH, INC., et al.

Plaintiffs,

v.

DR. SERGIO CHEVERE, et al.

Defendant.

CIV. NO. 12-1678(PG)

OPINION AND ORDER

Before the court are defendant Dr. Sergio Chevere's ("defendant")[1], and plaintiffs American Health, Inc. ("AHI"), Socios Mayores en Salud, Inc., and Socios Mayores en Salud Holding, Inc.'s (collectively, "plaintiffs") cross-motions for summary judgment, and both parties' responses thereto. See Docket Nos. 124, 125, 128 and 129. For the reasons specified below, summary judgment is **GRANTED** for defendant. Plaintiffs' motion for summary judgment is accordingly **DENIED**.

I. FACTUAL BACKGROUND

Defendant was a high-ranking employee at AHI and later worked for plaintiffs as a consultant. See Docket No.126 Plaintiffs' Statement of Uncontested Material Facts ("PSUMF") ¶¶ 4, 16 and 17. Between May 12 and May 14, 2012, defendant forwarded fifty-four e-mails from his business e-mail account to his personal e-mail account. See PSUMF ¶ 25. The business e-mail account was held in plaintiffs' private servers. See PSUMF ¶¶ 14 and 26. The forwarded e-mails had remained opened in defendant's business e-mail account inbox before defendant forwarded the same to his personal account. See Docket No. 126-5 (Plaintiff's Exhibit E) at page 12.

Defendant did not cause damage to or erase data from plaintiffs' computer systems. See Docket No.124-3 Defendant's Statement of Uncontested Material Facts ¶ 37. Plaintiffs claim the fifty-four e-mails contained confidential and proprietary information, but the court will make no findings of fact to that regard because such a finding would be immaterial to resolving the controversy before this court.

[1] Iraida del Rio and the Conjugal Partnership Chevere-Del Rio are also named as co-defendants.

Plaintiffs filed suit on August 20, 2012. They claim to have spent $178,568.73 from July 31, 2012 to March 31, 2016 in the litigation of the above-captioned case. See PSUMF ¶ 62. They submit to this court proof of billings payable to the law firm Casellas, Alcover & Burgos P.S.C. for legal fees in that exact amount. See Docket No. 126-9 (Plaintiff's Exhibit I). See also Docket No. 16-1.

Plaintiffs claim that defendant misappropriated proprietary and confidential information, in violation of federal and state law. Both parties now move for summary judgment in their favor.

II. STANDARD

Through summary judgment, courts "pierce the boilerplate of the pleadings and assay the parties' proof in order to determine whether trial is actually required." Wynne v. Tufts Univ. Sch. of Med., 976 F.2d 791, 794 (1st Cir. 1992). The Supreme Court encourages employing summary judgment in federal courts - it "[avoids] full blown trials in unwinnable cases, … [conserves] parties' time and money, and [permits] the court to husband scarce judicial resources." McCarthy v. Northwest Airlines, Inc., 56 F.3d 313, 314 (1st Cir. 1995). See also Celotex Corp. v. Catrett, 477 U.S. 317 (1986).

A court may grant summary judgment only when the pleadings and the evidence demonstrate that "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). See also Sands v. Ridefilm Corp., 212 F.3d 657, 660 (1st Cir. 2000). A factual dispute is "genuine" if it could be resolved in favor of either party, and "material" if it potentially affects the outcome of the case. See Calero-Cerezo v. U.S. Dep't of Justice, 355 F.3d 6, 19 (1st Cir. 2004). The court must review the record "taken as a whole," and "may not make credibility determinations or weigh the evidence." Reeves v. Anderson Plumbing Productions Inc., 530 U.S. 133, 135 (2000). Credibility determinations, the weighing of the evidence, and the drawing of legitimate inferences from the facts are functions of a jury, not of a judge. See id.

In short, when there is a genuine dispute as to any material fact, and when a court would be required to make credibility determinations, weigh the evidence, or draw legitimate inferences from the facts in order to adjudicate a controversy, summary judgment will not be granted. While no legitimate inferences can be drawn, the court will construe all reasonable inferences in favor of the nonmoving party. See Stoutt v. Banco Popular de Puerto Rico, 158 F. Supp. 2d 167, 171 (D.P.R. 2001). Still, the nonmoving party is required to demonstrate "through submissions of evidentiary quality that a trial worthy issue persists." Iverson v. City of Boston, 452 F.3d 94, 108 (1st Cir. 2006).

III. DISCUSSION

A. The Mise-En-Scène: An Overview of Malicious Cyber Acts and Plaintiffs' Claims

Cyber technologies are a minefield of technical nuances. Naturally, the legal landscape that affects cyberspace can be seemingly riddled with gray areas and be difficult to navigate. Before jumping into the proverbial Minotaur's maze, the court will, for clarity's sake, consider some introductory notes on malicious cyber acts.

It is well-settled that malicious cyber acts can lead to civil liability and criminal prosecution. Indeed, criminal enterprises, malign actors, and those seeking to gain unfair advantages in their ventures increasingly turn to cyberspace to carry out or facilitate malicious acts.

Put plainly, malicious cyber acts consist of the use of computer driven technologies to commit malicious acts. They can be parceled into three distinct categories: (1) acts in which a computer is the target of the malicious activity, (2) acts in which a computer is used as a tool that is essential for the malicious activity, and (3) acts in which the use of a computer is incidental to the malicious activity. These distinctions are important when applying the law to malicious cyber acts. The court will discuss the first and second categories in more detail, insofar as the latter is immaterial to the issue at hand.

Acts in the first category, in which a computer is the target, can ordinarily only exist in cyberspace (e.g. hacking and distributed denial of service attacks). They are an entirely "new" breed of malicious activity. Traditional statutes are often ill-fitted or otherwise insufficient to carry civil claims and criminal prosecutions addressing malicious cyber acts of this sort. Thus, to properly make malicious cyber acts that fall into the first category actionable, specialized statutes that specifically target conduct in cyberspace are necessary.

On the other hand, acts in the second category, in which a computer is an essential tool, are mostly age-old malicious acts (e.g. fraud and theft) being committed in new ways. They are, in that sense, "old wine in new bottles." Take, for example, a fraud committed in cyberspace and one committed in the physical world: both are fraud, but only the former is a malicious cyber act. They are different in that a computer was used as an essential tool in one but not in the other. A malicious cyber act falling into the second category can be properly addressed through a traditional statute, though specialized legislation could nonetheless streamline litigation or prescribe particular remedies. That is to say, while Congress could very well choose to enact legislation that specifically targets, say, instances of fraud committed through the use of a computer, traditional statutes addressing fraud could be perfectly adequate to carry the day.[2]

In the case at hand, plaintiffs allege that defendant engaged in the illegal misappropriation of confidential information. Such conduct would fall squarely within the second category of malicious cyber acts (i.e. acts in which a computer is used as a tool that is essential for the malicious activity). Hence, traditional laws may be more suitable conduits for plaintiffs legal action, rather than statutes that specifically target malicious cyber acts. In fact, Congress may well have intended such conduct to remain codified under traditional laws.

---

[2] The previous paragraphs paraphrase Chapter 2 of Ralph D. Clifford's Cybercrime: The Investigation, Prosecution and Defense of a Computer Related Crime. See Ralph D. Clifford, Cybercrime: The Investigation, Prosecution and Defense of a Computer Related Crime 15-20 (2011).

Plaintiffs set forth three federal question claims, pursuant to the Computer Fraud and Abuse Act (CFAA), the Wiretap Act, and the Stored Electronic Communications Act (SECA). These three statutes are not catch-all nets for malicious cyber acts. Instead, they target specific forms of conduct in cyberspace, under specific circumstances. For the reasons stated below, the court finds that defendant's alleged misappropriation of confidential information falls outside the purview of the CFAA, the Wiretap Act, and the SECA. Instead, the court finds that the remedies plaintiffs request are more properly sought under state law.

In addition to the federal causes of action, plaintiffs also raised supplemental claims under Puerto Rico's Industrial and Trade Secret Protection Act, as well as claims of breach of contract, breach of duty of loyalty, breach of implied contractual and legal duty, and conversion, all pursuant to Puerto Rico's Civil Code. These claims find their way to federal court through supplemental jurisdiction, on the back of plaintiffs' federal question claims.

B. A Chink in the Armor: The Computer Fraud and Abuse Act

Plaintiffs claim that defendant's alleged misappropriation of confidential information violates the CFAA. However, plaintiffs fail to cross the statutory damage threshold.

The CFAA proscribes that whoever "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value … shall be punished." 18 U.S.C. § 1030(a)(4). However, a civil claim can only be raised when the plaintiff suffers damage or loss amounting to $5,000 or more. See 18 U.S.C. § 1030(g). Here, plaintiffs did not.

The CFAA defines the term damage narrowly. Damage "means any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Certainly, the CFAA's definition of damage "does not encompass any harm resulting from the disclosure to a competitor of trade secrets or other confidential information." Sun W.

Mortg. Co., Inc. v. Matos Flores, No. CV 15-1082 (GAG), 2016 WL 1030074, at *4 (D.P.R. Mar. 10, 2016). In fact, damages under the CFAA are restricted to "the destruction, corruption, or deletion of electronic files, the physical destruction of a hard drive, or any diminution to the completeness of the system." New South Equip. Mats, LLC v. Keener, 989 F.Supp. 2d 522, 529 (S.D.Miss. 2013). It is patently clear that, while defendant may have acquired confidential information without plaintiffs' authorization, plaintiffs did not suffer any damage, as defined by the CFAA, because of the intrusion. It is uncontested that defendant caused no impairment to the integrity or availability of the data. No electronic files were destroyed, corrupted or deleted, nor was the completeness of the system diminished in any way.

Plaintiffs now hope to reach the threshold amount only by showing they suffered loss. They claim that "the evidence … establishes that to (1) assess the extent of Chevere's violation, (2) take remedial measures, and (3) prosecute this case AHI has incurred expenses to the tune of $178,568.73 since the inception of the case." Docket No. 128 at page 14.

In the context of the CFAA, loss means

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11). "Although the First Circuit Court of Appeals has held that the CFAA does not restrict 'loss' under the statute to purely physical damage, nothing in the statute suggests that the alleged loss or costs can be for matters unrelated to the computer." Padmanabhan v. Healey, 159 F. Supp. 3d 220, 224 (D. Mass. 2016), aff'd, No. 16-1159, 2017 WL 3404402 (1st Cir. Jan. 4, 2017) (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 584 (1st Cir.2001); Shirokov v. Dunlap, Grubb & Weaver, PLLC, 2012 WL 1065578, at *24 (D. Mass. Mar. 27, 2012)).

Following the aforementioned case law, costs incurred in conducting a damage assessment and repairing a damaged computer system count towards determining loss under the CFAA. The time spent by employees assessing

damage to or fixing a computer system also constitutes loss. However, the time spent by employees not carrying out tasks specific to the computer does not (such as a meeting to determine whether to file suit because of an intrusion). See Wilson v. Moreau, 440 F.Supp. 2d 81, 109 (D.R.I. 2006), aff'd, 492 F.3d 50 (1st Cir. 2007). Legal fees incurred by a plaintiff similarly cannot be used to satisfy the $5,000 threshold. See Wilson, 440 F.Supp. 2d 110. In short, loss encompasses costs incurred only when directly related to the computer and revenues lost due to an interruption of service.

The record evinces that plaintiffs have indeed spent $178,568.73 since the "inception of this case." Docket No. 128 at page 14. However, this amount accounts entirely for legal fees paid to the law firm that represents them in this case. See PSUMF ¶ 62 ("AHI has incurred expenses to the tune of $178,568.73 related to legal fees and costs in connection with its representation…"). As evidentiary support to satisfy the $5,000 statutory threshold amount, plaintiffs **only** submitted to the court proof of the fees they paid (and owe) to the representing law firm. See Docket No. 126-9 (Plaintiff's Exhibit I). See also Docket No. 16-1. As previously stated, costs incurred by plaintiffs due to legal fees do not constitute loss in the context of the CFAA. See Wilson, 440 F.Supp. 2d 110. The factual record plaintiffs submitted is devoid of other showings of loss that would push plaintiffs' claim over the statutory threshold amount. As such, plaintiffs' claim necessarily fails.

Some courts have held that "loss of confidential and proprietary information for the benefit of defendants' competing enterprise" constitutes loss in the context of the CFAA. Res. Ctr. for Indep. Living, Inc. v. Ability Res., Inc., 534 F.Supp. 2d 1204, 1211 (D.Kan.2008). See also Meats by Linz, Inc. v. Dear, 2011 WL 1515028 at *3 (N.D. Tex. Apr. 20, 2011). Other courts, including district courts in the First Circuit, have made a more restrictive reading of the statute, holding instead that such loss does not count towards the CFAA's statutory threshold. See Wilson, 440 F.Supp. 2d 110 ("revenues lost due to the unfair business competition resulting from the hacked confidential information did not count towards the 'loss' requirement")". See also Sun W. Mortg. Co., Inc. v. Matos Flores,

No. CV 15-1082 (GAG), 2016 WL 1030074, at *4 (D.P.R. Mar. 10, 2016); Nexans Wires S.A. v. Sark-USA, Inc., 319 F.Supp.2d 468, 471-477 (S.D.N.Y. 2004). The First Circuit Court of Appeals has yet to face the question squarely.

In any event, the court agrees with its sister court in Rhode Island: the use of confidential and proprietary information to the detriment of the plaintiff does not constitute loss in the context of the CFAA. See Wilson, 440 F.Supp. 2d 110. At any rate, the court need not reach that question because plaintiffs have failed to show that they suffered any injury due to the alleged misappropriation of confidential information. In fact, plaintiffs themselves rightly observe: "The only reason [defendant] can claim that he did not use AHI's confidential and proprietary information to the detriment of AHI, was because AHI moved quickly to enjoin him from using and disclosing such information to third parties." Docket No. 128 at page 8. In light of that concession, and of the absence of any showing of materialized damages, plaintiffs' CFAA claim is nothing short of an oxymoron. The court is bewildered that plaintiffs affirm to have suffered grave injury while conceding they dodged the bullet thanks to their swift action. Plaintiffs cannot have their cake and eat it too.

Because plaintiffs have failed to establish damage or loss amounting to $5,000, their CFAA claim necessarily fails, and defendant is entitled to summary judgment as a matter of law. No material facts relevant to the adjudication of this claim remain in question. Thus, plaintiffs' claim is DISMISSED WITH PREJUDICE.

C. Leaning on a Broken Reed: The Wiretap Act

Next, plaintiffs sustain that defendants violated the Wiretap Act. However, their reliance on this statute is wholly misguided. The alleged misconduct does not fall within the purview of the Wiretap Act.

The Wiretap Act punishes anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C.A. § 2511(1)(a). The statute provides for a civil cause of action. The Wiretap Act defines intercept as "the aural or other acquisition of the

contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Electronic communication "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce… ." 18 U.S.C. § 2510(12). The transfer of an e-mail, thus, would constitute an electronic communication.

It is not unlawful "for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication…" 18 U.S.C. 2511(d). However, the interception violates the Wiretap Act, despite the person being a party to the communication, when "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." Id. Thus, even if defendant was the recipient of the e-mails in question, he could still have violated the Wiretap Act if he forwarded the e-mails with the purpose of committing a criminal or tortious act – a question that is, at this point, very much in dispute.

The First Circuit Court of Appeals has not yet decided whether the Wiretap Act requires that an interception occur contemporaneously to the transmission of the electronic communication. Today, this court faces that issue head-on, where here (a) defendant forwarded the e-mails in question after transmission of the electronic communications had been completed and transit concluded, (b) the communications had been opened by the intended recipient, and (c) had remained opened in his inbox for some time.

"The Fifth Circuit and several others have approved the judicial definition of 'intercept' as acquisition contemporaneous with transmission." TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo, No. CV 15-2121 (BJM), 2017 WL 3242244, at *4 (D.P.R. July 28, 2017)(citing Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002); Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994)). "These circuits have distinguished between materials acquired in transit, which are interceptions, and those acquired from storage, which purportedly

are not." In re Pharmatrak, Inc., 329 F.3d 9, 21 (1st Cir. 2003)(citing Konop, 302 F.3d at 878). While caselaw from other circuits is not controlling here, it is certainly persuasive.

Thus, following these decisions, this court agrees that:

> the interception must occur while the communication is transmitted, or the conduct may fall instead under the provisions of the Stored Wire and Electronic Communications Act, which prohibits access and disclosure of information stored electronically. However, it is difficult to determine when a communication is "in transit" because electronic communications, such as e-mails or voice-mails, are only transmitted for milliseconds and stored on different servers as they are routed.

Ralph D. Clifford, Cybercrime: The Investigation, Prosecution and Defense of a Computer Related Crime 215 (2011).[3] This finding disposes of plaintiffs' Wiretap Act claim. The e-mails in question had been delivered, opened by the recipient, and stored in the recipient's inbox for some time until they were accessed and forwarded by defendant. Thus, it is patently obvious to this court that the communications were no longer "in transit," but had rather "crossed the finish line of transmission." Accordingly, the alleged "interceptions" did not occur contemporaneously to the transmission of the original e-mail messages. Their subsequent forwarding, which is the object of defendant's alleged breach, does not fall under the purview of this particular act.

In short, this court finds that the acquisition of an electronic communication must occur contemporaneously to the transmission thereof in order to constitute an interception within the context of the Wiretap Act. Defendant allegedly acquired the electronic messages in question to his

[3] In Councilman, the First Circuit of Appeals faced the question of whether an e-mail was an electronic communication when stored temporarily in a server that acts merely as a conduit for routing the e-mail to its final destination. Ruling *en banc*, the Court decided that "the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications." U.S. v. Councilman, 418 F.3d 67, 79 (1st Cir.2005). But, given that neither the facts nor the arguments presented in Councilman "invite[d] consideration of either the existence or the applicability of a contemporaneity or real-time requirement" the Court did "not plunge into that morass." Councilman, 418 F.3d 80. Here, the court cannot side-step considering the existence of a real-time requirement for intercepting an electronic communication in the context of the Wiretap Act.

personal e-mail after transmission to his business e-mail had concluded, when acquisition could no longer be considered interception. As such, plaintiffs' claim stands a snowball's chance in hell of succeeding, since acquiring an electronic communication after transmission has concluded cannot violate the Wiretap Act. Defendant is entitled to judgment as a matter of law, and no material facts relevant to the adjudication of this claim remain in question. Plaintiffs' claim is thus DISMISSED WITH PREJUDICE.

D. A Flash in the Pan: The Stored Electronic Communications Act

The court now turns to plaintiffs' SECA claim. The SECA protects electronic communications that are not in transit and instead lie in electronic storage. However, the SECA's framework is highly technical, and its scope much narrower than plaintiffs suggest. Hence, while plaintiffs claim that defendant's alleged misappropriation of certain e-mail messages containing confidential information violates the SECA, the court finds that defendant's actions do not fall within the statute's limited scope.

Whoever "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system" violates the SECA. 18 U.S.C. § 2701(a). A person aggrieved by a violation of the SECA may seek civil remedy through a private right of action. See 18 U.S.C. § 2707(a). However, defendant did not violate § 2701(a) because the e-mails in question were not in electronic storage in the context of the SECA at the time they were allegedly misappropriated.

The SECA defines the term "electronic storage" narrowly. The term does not apply to all storage of electronic communications. Instead, "electronic storage" means "(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication

service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

When the intended recipient opens an e-mail and chooses to keep that e-mail in the inbox server, that opened e-mail is not held in electronic storage as defined by the SECA. See Fraser v. Nationwide Mut Ins. Co., 135 F.Supp. 2d 623, 635-36 (E.D.Pa.2001), aff'd in part, 352 F.3d 107, 114 (3d Cir.2004). See also United States v. Weaver, 636 F.Supp 2d 769, 772-773 (C.D.Ill.2009); Bansal v. Russ, 513 F.Supp. 2d 264, 276 (E.D.Pa. 2007) (holding that accessing opened e-mail does not violate the SECA). Opened e-mail that remains stored in an inbox server is not held in electronic storage because it is not in "temporary, intermediate storage" that is "incidental" to transmission, nor is it acting "for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

In Theofel, the Ninth Circuit held that previously accessed e-mails are in electronic storage because they offer backup protection. See Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir.2004)(although conceding that opened e-mail does not function as a backup, and is thus not in electronic storage, when stored only in a Remote Computing Service). However, this court finds Theofel unpersuasive. See generally Jennings v. Jennings, 401 S.C. 1 (2012)("We decline to hold that retaining an opened e-mail constitutes storing it for backup protection under the Act."). "The Ninth Circuit's interpretation of storage for backup protection under the Stored Communication Act cannot be squared with legislative history and other provisions of the Act." Weaver, 636 F. Supp. 2d, 772.

> Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by section 2702(a)(2).

H.R.Rep. No. 99–647, at 65 (1986). Section 2702(a)(2) refers to the treatment of material held in a Remote Computing Service. See 18 U.S.C. § 2702(a)(2).

The SECA distinguishes between electronic communications that are stored by an Electronic Communications Service (ECS) and a Remote Computing Service (RCS). An ECS is "any service which provides to the users thereof the ability to send or receive wire or electronic messages." 18 U.S.C. § 2510(15). Meanwhile, a system constitutes an RCS when it engages in "the provision to the public of computer storage or processing service by means of an electronic communications system." 18 U.S.C. § 2711(2). "The classifications of ECS and RCS are context sensitive: the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract." Orin Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev 1208, 1215 (2004).[4]

When a user leaves previously opened e-mail in an inbox server, the service provider acts as an RCS, rather than an ECS, with respect to that particular electronic communication. See id. at 1217. See also Prosecuting Computer Crimes, DOJML Comment 9-3.000, 5 Department of Justice Manual (Supp.2011-13)(citing H.R.Rep. No. 99–647, at 65 (1986)). As such, defendant could not have violated § 2701(a) because that section of the SECA does not apply to materials held in an RCS. To boot, not even the RCS rules apply to plaintiffs' data because American Health Inc.'s private servers constitute a non-public service provider. An RCS must provide "to the *public* … [a] computer storage or processing service." 18 U.S.C. § 2711(2) (emphasis ours).

Plaintiffs' SECA claim is without merit because the e-mails in question were not in electronic storage as required by § 2701(a) at the time the alleged misappropriation took place. Furthermore, the e-mails in question were stored in a non-public service provider acting as an RCS. As such, defendant is entitled to judgment as a matter of law. No material facts

[4] In Theofel, the Ninth Circuit maintained that a service provider could act as both an ECS and an RCS simultaneously. See Theofel, 359 F.3d 176-177. However, this court rejects that holding. The provisions that apply to ECS and RCS are mutually exclusive. Indeed, "if an e-mail message is covered by both the ECS and RCS rules at the same time, the legal process that is permitted under the RCS rules would violate the ECS rules." Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, at Footnote 61.

relevant to the adjudication of this claim remain in controversy. Thus, plaintiffs' SECA claims are DISMISSED WITH PREJUDICE.

E. Stacked on Pillars of Sand: Plaintiffs' State Law Claims

Plaintiffs' remaining claims rely on state law, and found their way to federal court through supplemental jurisdiction.

When all federal claims are dismissed, the court typically declines to exercise supplemental jurisdiction over a plaintiff's state law claims. See Camelio v. American Federation, 137 F.3d 666, 672 (1st Cir. 1998)("Certainly, if the federal claims are dismissed before trial, … the state claims should be dismissed as well."); Rodriguez v. Doral Mortgage Corp., 57 F.3d 1168, 1177 (1st Cir.1995).

This court has already disposed of plaintiffs' federal claims. As such, it will no longer exercise supplemental jurisdiction over plaintiffs' state law claims. As a result, all of plaintiffs' state law claims are DISMISSED WITHOUT PREJUDICE.

IV. CONCLUSION

For the foregoing reasons, defendant's motion for summary judgment is **GRANTED**, insofar as plaintiffs' federal question claims are without merit, and defendant is entitled to judgment as a matter of law. Plaintiffs' motion for summary judgment is accordingly **DENIED**. Plaintiffs' federal question claims are thus **DISMISSED WITH PREJUDICE**. As such, this court will no longer exercise supplemental jurisdiction over plaintiffs' remaining claims. Thus, plaintiffs' state law claims are **DISMMISSED WITHOUT PREJUDICE**. Judgment will be entered accordingly.

IT IS SO ORDERED.

In San Juan, Puerto Rico, December 22, 2017.

S/ JUAN M. PÉREZ-GIMÉNEZ
JUAN M. PEREZ-GIMENEZ
SENIOR U.S. DISTRICT JUDGE